Best Practices in Risk-Based Internal Auditing

by Sheryl Vacca

Executive Summary

- Agree on a common framework for the risk-based auditing and monitoring program.
- Assess risks across the enterprise and then prioritize them by looking at the likelihood of occurrence and impact for the organization.
- Develop a risk-based auditing and monitoring plan from the identified risk priorities.
- Execute a corrective action plan developed by management to mitigate risks and/or resolve risks.
- Assess the auditing and monitoring process for effectiveness.

Getting Started

In designing risk-based auditing and monitoring activities, it is important that the internal auditor works closely with the organization's senior leadership and the board, or committee of the board, to gain a clear understanding of auditing and monitoring expectations and how these activities can be leveraged together to help minimize and mitigate risks for the organization. These discussions should also include leadership from the legal, compliance, and risk management functions, if they are not already a part of the senior leadership team.

This process should include performing periodic audits to determine compliance with respect to applicable regulatory and legal requirements, and to provide assurance that management controls are in place for the detection and/or prevention of noncompliant behavior. Additionally, risk-based auditing and monitoring should include mechanisms to determine that management has implemented corrective action through an ongoing performance management process to address any noncompliance.

Once the common framework for the risk-based auditing and monitoring program has been established, four key tasks must be performed:

1. Assessment and prioritization of risks, conducted enterprise-wide;
2. Development of a risk-based auditing and monitoring plan;
3. Execution of a corrective action plan developed by management to mitigate risks and/or resolve risks;
4. Periodic assessment of the overall process for effectiveness.

Risk Assessment

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) helped to define "risk" as any event that can keep an organization from achieving its objectives.[1] According to the COSO model, risk is viewed in four major areas:

- operational (processes and procedures);
- financial (data rolling up to internal/external statements);
- regulatory (federal, state, local, organizational policy);
- reputation (institutional).

There are several ways in which risk assessments in these areas can be conducted. These include the use of:

- focus groups to assist in the identification of risks;
- interviews of key leadership and the board;
- surveys;
- reviews of previous audit findings, external audits conducted in the organization, and identifying what is occurring within the industry and the local market, etc.

Once risks have been identified, a prioritization process is needed to identify the likelihood of the risk occurring, the ability of management to mitigate risk (i.e. are there controls in place for risk, regardless of

the likelihood of those risks of occurring?), and the impact of risk on the organization. Risk prioritization is an ongoing process and should include periodic reviews during the year to ensure that previous prioritization methods, when applied in real time, are still applicable for the risk.

It is important that senior leadership participate in, and agree with, the determination of the high-risk priorities for the audit and monitoring plan. This will ensure management buy-in and focus on risk priorities. Also, with managers involved at the development stage of the plan, they will be educated as to the type of activities being planned and the resources needed to conduct these activities. Hence, during the plan year, if there are changes, management will understand the need for additional resources or a change in focus in the plan as the business environment and priorities may change.

Developing the Plan

The International Standards for the Professional Practice of Internal Audit (IIA), Standard 2120 says "The internal audit activity must evaluate the effectiveness and contribute to the improvement of the risk management processes." [2]

This is done through the development and execution of the risk-based auditing and monitoring plan.

Risk assessments and prioritization are important elements in the development of your risk-based auditing and monitoring plan. Considerations related to the plan should also include:

- Review of other business areas in the organization which may be conducting an audit or monitoring activity in this area:
  - If so, could you leverage this resource for assistance in completing the stated activity, or utilize their activity and integrate the results into the overall plan?
- Resources available to implement plan:
  - Do you have the appropriate resources for the subject matter as needed within your department? (If not, is there subject matter expertise somewhere else in the organization?)
  - If subject matter requires outsourcing, budget considerations and overall risk priorities may need to be re-evaluated.
- Hours needed to complete the plan
- Projected timeframes
- Defined auditing or monitoring activities and determination as to whether they are outcomes or process oriented
- Flexibility incorporated into the plan to address changes in risk priorities and possibly unplanned compliance risks/crises which may need an immediate audit or monitoring to occur.

IIA Standard 2120.A1 identifies the focus of the risk assessment process: "The internal audit activity must evaluate risk exposures related to the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.
- Safeguarding of assets;
- Compliance with laws, regulations, and contracts.

The process of risk assessment continues through the execution of the plan where the engagement objectives would reflect the results of the risk assessment. Risk-based auditing and monitoring is ongoing and dynamic with the needs of the organization.

Execution of the Plan—Making It Happen

Each activity should have a defined framework which will provide management with an understanding of the overall expectations and approach as you execute the plan. The framework for your activities should include the following actions:

- Set the purpose and goal for the activity (audit or monitoring):

  - Identify the scope from the purpose or goal, but make sure that it is objective, measurable, and concise.
  - Before conducting activities in high-risk priority areas, it is important to consider whether legal advice may be needed in establishing the approach to the activity.
- Conduct initial discussion with the business area for input related to audit attributes, timing, and process:
  - Concurrent vs retrospective status may be determined at this point. (Concurrent is “real time” and before the end point of what you are looking at has occurred. Retrospective is after the end point has occurred, i.e. the claim has been submitted or the research has concluded, etc. Milestones should be determined for rationale as to how far back to go, for example, new law, new system, etc.)
- Finalize the approach and attributes:
  - Sampling methodology will be determined largely by the scope (purpose and goal) of your activity. For example, the sample used in self reporting a risk area to an outside enforcement agency may be predetermined by the precedent that the enforcement agency has set in industry; to determine if education is needed in a risk area, a small sample only may be needed, etc.
  - Consider the audience frame of reference that will receive the results of activity, and then develop an appropriate format for reporting.
- Conduct the activity.
- Identify preliminary findings and observations.
- Provide an opportunity for findings and observations to be validated by the business area.
- Finalize the report.
- Identify processes for the follow-up after management has taken corrective action related to activity findings and observations.
  - Data collection and tracking are critical because they provide trend analysis and measurement of progress.
- Determine the key points of activity that may be provided to leadership and/or in reporting to the board.

The overall process of developing the audit and monitoring plan should be documented. This would include a description of how the risk assessment was conducted and the methodology for prioritization of risks. Working papers to support the audit findings, reports, and corrective action plans should be documented and filed appropriately. Prior to the audit activity, be sure to define and document what should be considered as part of the working papers.

At the end of each plan year, it is important to conduct an evaluation of the overall effectiveness of the plan. Questions to consider may include:

- Was the plan fully executed?
- Were appropriate resources utilized for the plan’s execution?
- Were the activities conducted in a timely manner?
- Did the plan “make a difference” in regard to the organization’s strategy and business?
- Did the plan reach the goal of detecting, deterring, and/or preventing compliance research risks from occurring?

Annual evaluations may be conducted through self reviews or independently of the internal audit function by a third party, i.e. peer review conducted with auditors from other organizations, Quality Assessment Review conducted according to IIA standards (every 5 years), etc. However, while self reviews are less resource intensive, it is recommended that a independent review be conducted at least every other year to assess the effectiveness of your auditing and monitoring efforts. Figure 1 helps to identify the benefits of an effectively executed risk-based auditing and monitoring plan.

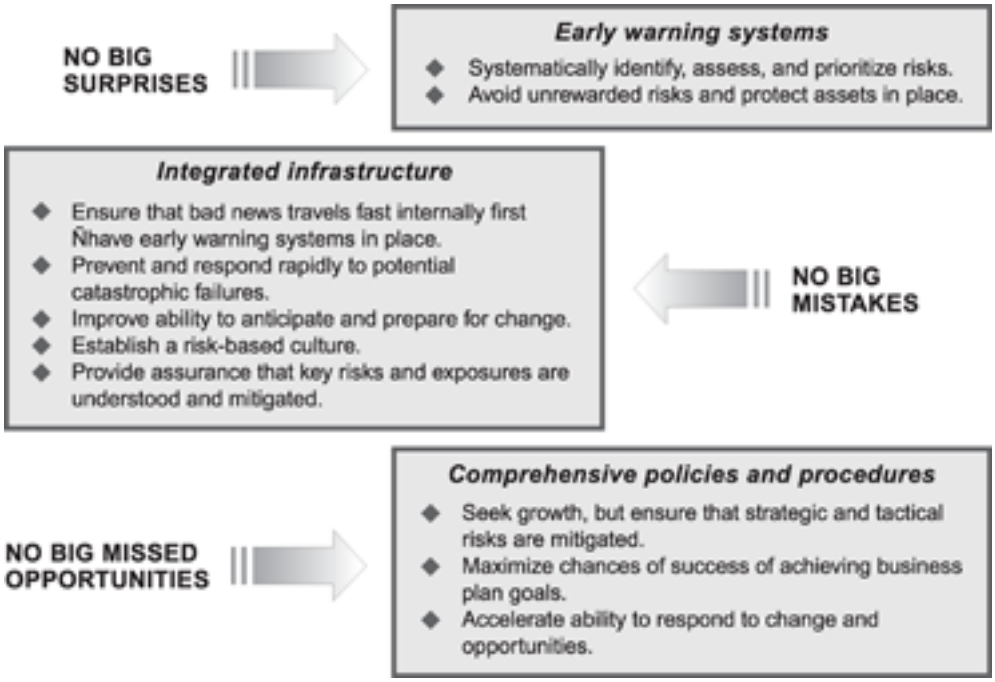

Figure 1. Benefits of an effectively executed risk-based auditing and monitoring plan

In summary, effectiveness in the development and execution of the risk-based audit and monitoring plan will be determined by the integrity and characteristics of the overall audit and monitoring process. Effective audit and monitoring activities will assist in the identification of weaknesses in controls, management's action to correct those weaknesses, and follow-up to ensure that timely mechanisms have been put in place to strengthen controls for mitigating the business risks. Additionally, risks will be detected, deterred and/or prevented with effective auditing and monitoring activities.

Case Study

Scenario: An organization with multiple businesses in several geographic locations is conducting an enterprise-wide risk assessment. It is noted during the risk assessment that, due to recent financial losses, the organization is going through a consolidation of business units and reduction in force. This has been identified as a high-risk priority area for the auditing and monitoring plan for the next fiscal year.

In planning the audit on the risk area of business consolidation, the following considerations should be included:

- The business consolidation could be impacting the organization in various ways—customer base loss, reduced finances, loss of reputation, loss of workforce resulting in loss of controls, etc.
- The risk-based audit will focus on areas of greatest impact: loss of controls in financial areas due to the reduction in workforce.
- The timing of the audit will be negotiated to bring the most value to the organization. This might involve having a two-part audit. Part I could take place after the business consolidation and reduction in workforce have occurred. This would include assessing the consolidated business unit to determine if there are any gaps in the financial controls. For instance, segregation of duties is commonly found in situations with loss of people and consolidation of functions. Any gaps identified would become actions for management to correct before the Part II audit took place.
- Management may also want to set up its own monitoring system to ensure that its corrective actions have resolved any of the gaps identified.
- Part II of the audit would occur after a negotiated period of time with management and would allow the corrective actions to have been in place long enough for their effectiveness to be determined.

The overall purpose of this type of risk-based auditing is to work with management in "real time," to add value to the organization in regard to its strategic and best business interest, and to provide input on

processes before they become “fixed.” After management believes it has the “fixes” in place, then the second part of the audit will help to provide assurances that the risks identified are no longer risks and that no new gaps or lack of controls have developed around the process of business consolidation and reduction in workforce.

Making It Happen

The development of an effective risk-based auditing and monitoring program includes several key elements:

1. Performing an enterprise-wide risk assessment that includes operational, financial, regulatory, and reputational risk (1-IIA).
2. Prioritizing risks identified through measures such as likelihood and impact for the organization.
3. Developing a risk-based auditing and monitoring plan from the identified risk priorities.
4. Determining that corrective action plans which have been developed by management to mitigate priority risks or ensure controls are in place to lower the risk level for the organization.
5. Conducting follow-up activities that validate, monitor, or audit corrective actions to mitigate and/or resolve the identified risks.
6. Re-evaluating risks on an annual basis through a risk assessment process to ensure that the priority risks of the organization have been addressed.
7. Conducting a periodic third-party review of risk-based auditing and monitoring plan to assess whether:
    a. processes are in place to identify risks;
    b. appropriate resources are utilized to audit and/or monitor risks;
    c. a commitment to reinforcing the need for management to execute plans to mitigate risks is demonstrated by the board and senior management.

More Info

Websites:

- Federal Sentencing Guidelines, Chapter 8. US Sentencing Commission’s webpage’s at www.ussc.gov/general.htm (history and overview of the guidelines) and www.ussc.gov/GUIDELIN.HTM (guidelines and manuals). Chapter 8’s provisions can be found at www.ussc.gov/2004guid/tabconchapt8.htm
- General Accounting Office (GAO): www.gao.gov
- Institute of Internal Auditors www.theiia.org
- Public Company Accounting Oversight Board (PCAOB): www.pcaobus.org
- Sarbanes–Oxley Act 2002: www.soxlaw.com
- Securities and Exchange Commission: www.sec.gov
- Society of Corporate Compliance and Ethics (SCCE): www.corporatecompliance.org

Notes

[1] The Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management Framework: Draft (2003).* Published in 2004 as *Enterprise Risk Management—Integrated Framework* and available from www.coso.org

[2] Institute of Internal Auditors. Professional Practice Standards 2120-Risk Management and Section A1., January, 2009.

See Also

Best Practice

- The Assurance versus Consulting Debate: How Far Should Internal Audit Go?
- The Effect of SOX on Internal Control, Risk Management, and Corporate Governance Best Practice
- Internal Auditors and Enterprise Risk Management

- New Assurance Challenges Facing Chief Audit Executives
- Optimizing Internal Audit
- Risk Management: Beyond Compliance
- What Is the Range of the Internal Auditor's Work?

Checklists

- Defining Corporate Governance: Its Aims, Goals, and Responsibilities
- Requirements of the UK Combined Code on Corporate Governance
- Understanding and Calculating the Total Cost of Risk
- Understanding Internal Audits

Finance Library

- Mastering Risk, Volume 1: Concepts

To see this article on-line, please visit
http://www.qfinance.com/auditing-best-practice/best-practices-in-risk-based-internal-auditing?full